

Symantec

Exam 250-530

Administration of Symantec Network Access Control 12.1

Version: 6.1

[Total Questions: 220]

Topic 1, Volume A**Question No : 1 - (Topic 1)**

Which two databases are supported when Symantec Endpoint Protection Manager is being configured? (Select two.)

- A. Oracle Database 11g
- B. Microsoft SQL Server 2005, SP2
- C. Microsoft SQL Express, SP1
- D. Microsoft SQL Server 2008
- E. MySQL Database 5.5

Answer: B,D

Question No : 2 - (Topic 1)

A guest is unable to download the On-Demand client. The guest is running Windows 7 64-bit and connecting with the Mozilla Firefox browser. The computer has 512 MB RAM and 50 MB free disk space. What is the likely cause of the problem?

- A. The guest's system has insufficient disk space.
- B. The guest's browser is unsupported.
- C. The guest's operating system is unsupported.
- D. The guest's system has insufficient RAM.

Answer: A

Question No : 3 - (Topic 1)

In an Enforcer command line interface, which filter is used to capture communication traffic between an Enforcer and a Symantec Endpoint Protection Manager?

- A. auth
- B. client
- C. query
- D. spm

Answer: D

Question No : 4 - (Topic 1)

Which log contains IP address, connection attempt, port information, and the direction of the connection?

- A. Enforcer Client log
- B. Enforcer Kernel log
- C. Enforcer Traffic log
- D. Enforcer Packet log

Answer: C

Question No : 5 - (Topic 1)

An organization has deployed Symantec Network Access Control with LAN Enforcer. Historically, all clients were Windows based endpoints. Now, Linux endpoints that authenticate with Microsoft Active Directory will need to be authenticated through the LAN Enforcer. Which entry needs to be added to the Switch Profile Action table to open the port for Linux endpoints once they have been authenticated through Active Directory user credentials?

- A. Host Authentication: Pass, User Authentication: Pass, Policy Check: Pass, Action: Open Port
- B. Host Authentication: Fail, User Authentication: Fail, Policy Check: Ignore, Action: Close Port
- C. Host Authentication: Unavailable, User Authentication: Pass, Policy Check: Unavailable, Action: Open Port
- D. Host Authentication: Pass, User Authentication: Unavailable, Policy Check: Unavailable, Action: Close Port

Answer: C

Question No : 6 - (Topic 1)

How can an administrator provide computers on a quarantine VLAN with access to

remediation materials without using static routes?

- A. Assign a virtual IP address to the NIC on the remediation server and add it to the quarantine VLAN.
- B. Create a static route from the quarantine VLAN to the Symantec Endpoint Protection Manager in the Enforcer command line interface.
- C. Multi-home the remediation server and connect one NIC to a port assigned to the quarantine VLAN.
- D. Put a wireless access point on the quarantine VLAN to provide wireless access to quarantined clients.

Answer: C

Question No : 7 - (Topic 1)

The 802.1x protocol has three major components: Supplicant, Authenticator and Authentication Server. Which elements serve each of these components when Symantec Network Access Control is being configured to use LAN Enforcement?

- A. Supplicant: Symantec Endpoint Protection Client,
Authenticator: Symantec LAN Enforcer,
Authentication Server: Microsoft Active Directory Domain Controller
- B. Supplicant: Microsoft Supplicant,
Authenticator: 802.1x Enabled Switch,
Authentication Server: Symantec LAN Enforcer
- C. Supplicant: Network Access Control Client,
Authenticator: Symantec Endpoint Protection Policy Manager,
Authentication Server: Symantec LAN Enforcer
- D. Supplicant: Microsoft Supplicant,
Authenticator: Microsoft Active Directory Domain Controller,
Authentication Server: Symantec Endpoint Protection Manager

Answer: B

Question No : 8 - (Topic 1)

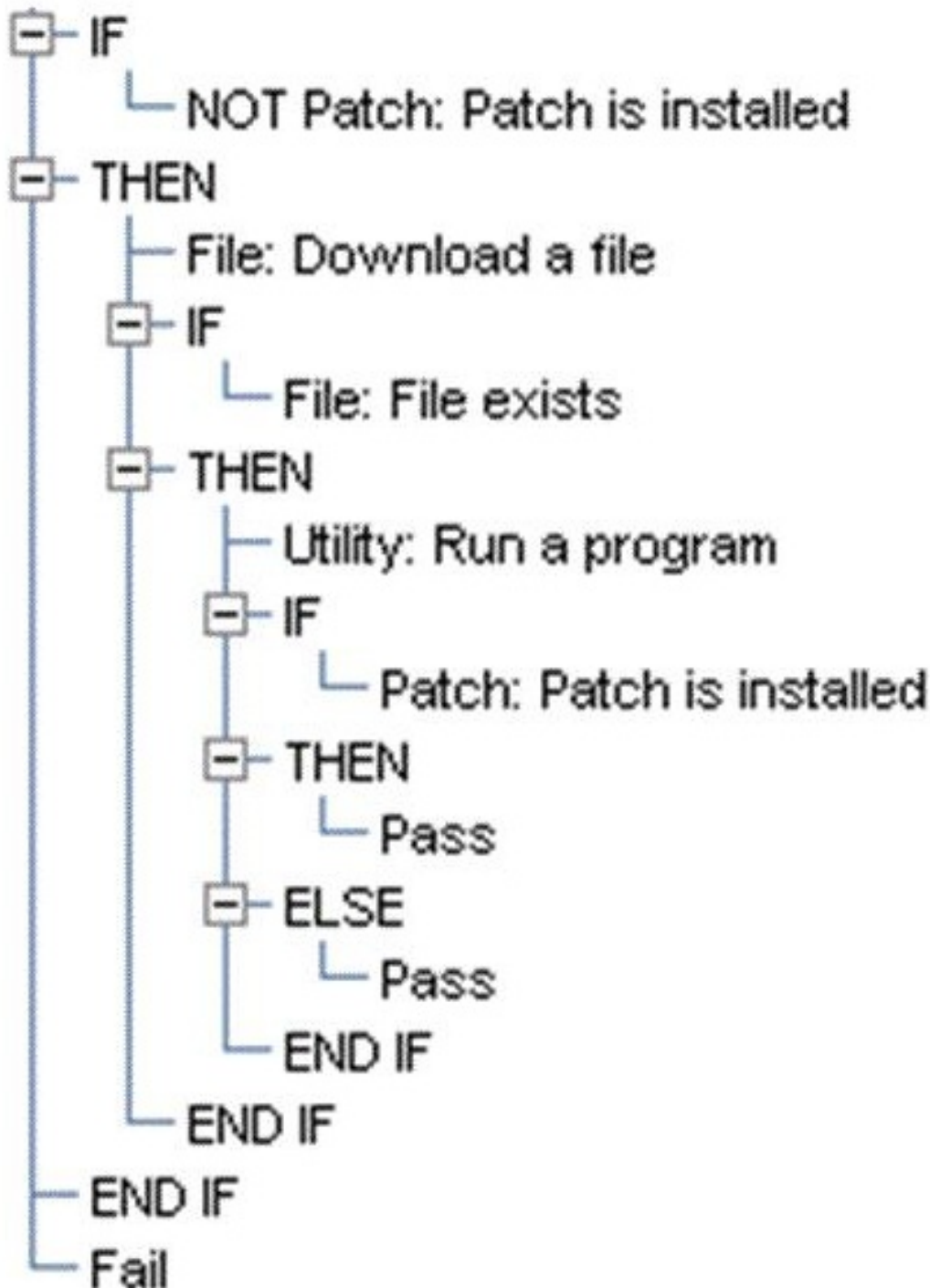
A Host Integrity policy has a complex custom conditional check that has three IF THEN statements, two of which have ELSE statements. How many ENDIF statements are required?

- A. 0
- B. 1
- C. 3
- D. 5

Answer: C

Question No : 9 - (Topic 1)

Refer to the exhibit.



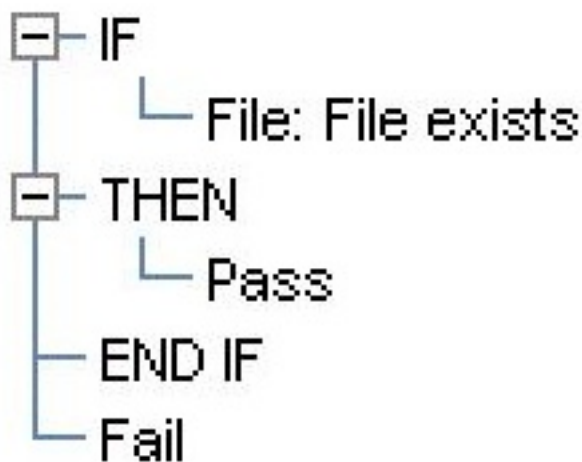
An administrator has created a custom requirement to remediate an operating system patch. The custom requirement appears to be working intermittently with clients that fail the patch installation, passing the requirement anyway. What is the likely cause of the issue?

- A. The logic is missing a Fail result.
- B. The logic is missing an ELSE statement.
- C. The logic has an extra Pass result.
- D. The logic needs an additional IF/THEN item.

Answer: C

Question No : 10 - (Topic 1)

Refer to the exhibit.



An administrator needs a custom requirement to run a script if a file does not exist. Which modification to the logic shown in the exhibit performs this functionality?

- A. Add a nested AND/OR statement to run a script after the END IF.
- B. Add a nested result to run a script after the Pass.
- C. Use an OR modifier to run a script after the IF.
- D. Use an ELSE statement to run a script after the THEN.

Answer: D

Question No : 11 - (Topic 1)

An organization with a Gateway Enforcer behind a VPN concentrator that is performing NAT, determines that clients are being blocked. What is the most likely cause of the problem?

- A. The client is missing from the MAC Address Bypass list.
- B. The IP address of the internal interface of the VPN connector needs to be added to the Trusted External IP Address list.
- C. The Enforcer is placed in the wrong physical location on the network.
- D. Static routes need to be added to the Symantec Endpoint Protection Manager to pass

the client traffic.

Answer: B

Question No : 12 - (Topic 1)

When a Gateway Enforcer is being deployed, which port needs to be kept open between the clients and the Enforcer?

- A. TCP 1812
- B. TCP 39999
- C. UDP 39999
- D. UDP 1812

Answer: C

Question No : 13 - (Topic 1)

How can access be permitted to remediation services when a client fails the Host Integrity check using a Gateway Enforcer?

- A. Add the client's IP address to the Trusted External IP Address List.
- B. Add the client's MAC Address to the Mac Address Bypass table.
- C. Add the IP addresses of the hosts to the Trusted Internal IP Address List.
- D. Add the client to the Allowed Client table on the Enforcer.

Answer: C

Question No : 14 - (Topic 1)

How does Symantec Network Access Control handle location switching compared to Symantec Endpoint Protection?

- A. It uses a reverse logic structure.
- B. It excludes locations.
- C. It uses locations instead of groups.
- D. It handles locations in the same way.

Answer: D

Question No : 15 - (Topic 1)

What will happen if a user switches to a location with a different Host Integrity policy while a Host Integrity check is in progress?

- A. The Host Integrity check will fail and the client will be denied network access.
- B. The client will stop the check and the user may get a timeout if attempting to reach remediation resources.
- C. The client is permitted guest access to the quarantine network until the next scheduled Host Integrity check.
- D. The Host Integrity check always completes prior to moving between locations.

Answer: B

Question No : 16 - (Topic 1)

Which two are explanations of why auto-location switching may be useful for Host Integrity? (Select two.)

- A. It can define different Remediation sources, based on location.
- B. It can enable different Antivirus features, based on location.
- C. It can choose different Firewall rule sets, based on location.
- D. It can select different Host Integrity checks, based on location
- E. It can enable different LiveUpdate features, based on location.

Answer: A,D

Question No : 17 - (Topic 1)

When would the Enforcer need to be reset to factory defaults?

- A. to change the type of Enforcer
- B. to upgrade the Enforcer
- C. to purge any errors on the Enforcer
- D. to purge all logs from the Enforcer

Answer: A

Question No : 18 - (Topic 1)

Which protocol is used to transfer packet captures from an Enforcer?

- A. FTP
- B. HTTP
- C. TFTP
- D. SFTP

Answer: C

Question No : 19 - (Topic 1)

What is the default time interval for Host Integrity checks?

- A. Continuous
- B. 2 minutes
- C. 5 minutes
- D. 30 minutes

Answer: B

Question No : 20 - (Topic 1)

An organization's security policy requires Host Integrity checks to run only when the client is connecting through a VPN concentrator whose internal interface is attached to a Gateway Enforcer. Which setting should be configured to only check Host Integrity on these external clients, but not check clients on the local network?

- A. Apply the Host Integrity agent to the external computers only.
- B. Add the IP addresses of the internal clients that need not be checked to the "Trusted Internal IP Address Range".
- C. Select "Only do Host-Integrity checking through the Gateway or DHCP Enforcer".
- D. Block port UDP 39999 on the client firewalls of the internal clients, so that they cannot be challenged by the Enforcer.